NEXTGEN@ICANN85 - INDIA - 2026

FAKE JOBS, REAL HARM: HOW DNS ABUSE TARGETS YOUNG JOB SEEKERS.

Rupam Barui
NextGen@ICANN85 Participant
National Forensic Sciences University

WHAT/WHO ¯_(ツ)_/¯

192.0.43.7

This is ICANN

This is not ICANN anymore

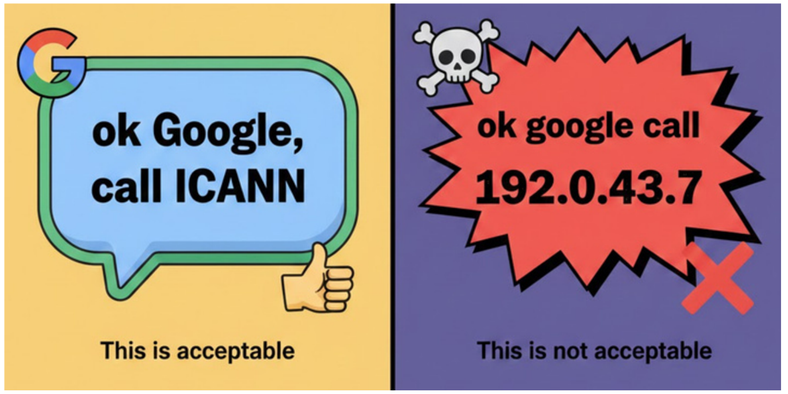
WWW.IANA.ORG

192.0.43.8

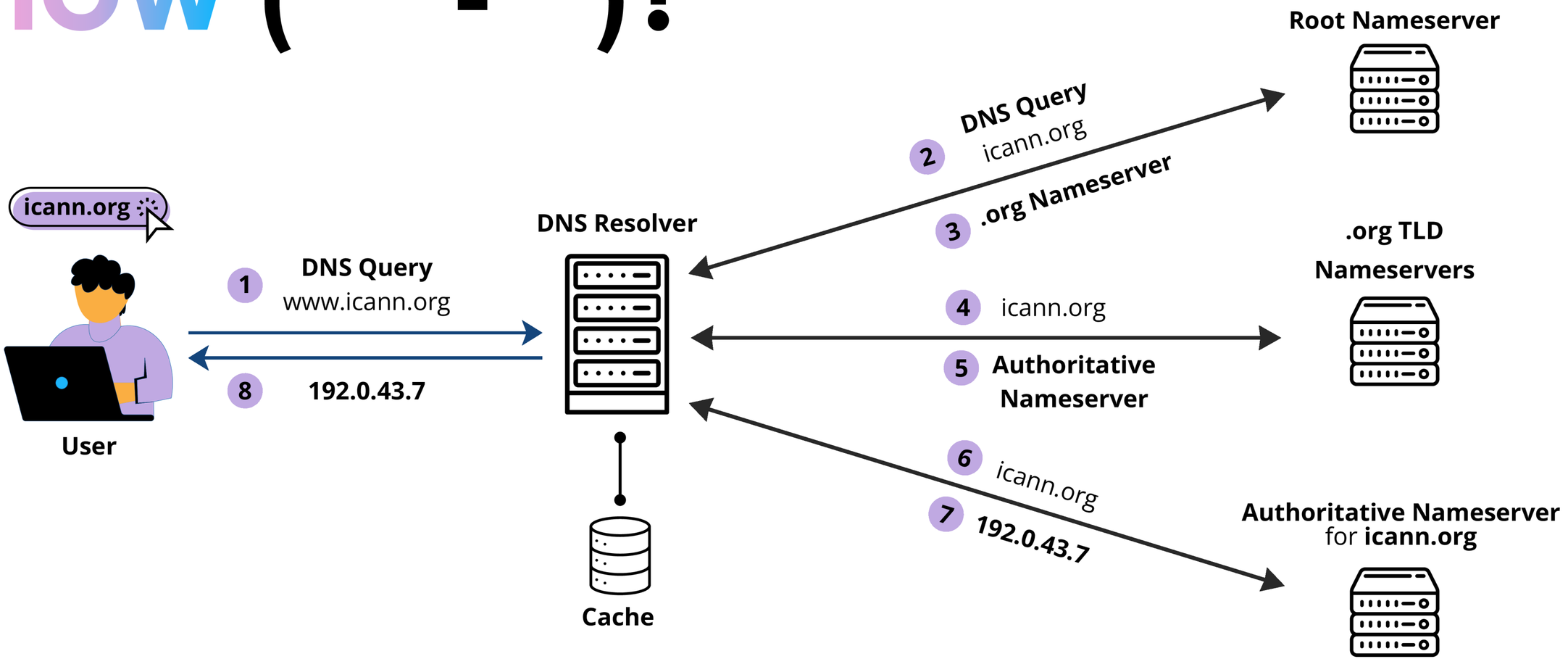
Single Mis - type

WHY WE DEPEND ON NAMES?

- IP addresses are **hard** to remember
- Humans rely on names and DNS makes this possible
- DNS converts domain names into IP addresses
- ICANN **coordinates** the global Internet's unique identifier systems, including the DNS root and top-level domains, to help ensure the **stable and secure** operation of the Internet.



HOW (' - ')?


Root Nameserver
DNS Query
icann.org
2
.org Nameserver
3
icann.org
DNS Resolver
.org TLD
Nameservers
1
DNS Query
www.icann.org
4
icann.org
5
Authoritative
Nameserver
8
192.0.43.7
6
icann.org
7
192.0.43.7
Authoritative Nameserver
for icann.org
User
Cache

https://jobs.rnicrosoft.com

Can you find anything wrong here

HTTPS://WWW.GOOGLE.COM

This is not a “m”

https://jobs.rnicrosoft.com

These are types of Homographic attacks

https://www.g00gle.com

These are not “o”s,
Rather “Zeros [0]”

THIS IS DNS ABUSE

DNS abuse refers to the use of domain names and DNS infrastructure to enable harmful activities such as:

Domain Impersonation	**Look-alike domains designed to trick users.**
Phishing Infrastructure	**Domains used to steal credentials and personal data.**
Malware Hosting	**Domains distributing malicious files or payloads.**
Botnet Command & Control	**Domains controlling infected devices.**
Spam & Scam Campaigns	**Domains used to spread large-scale fraud.**

WHAT THIS MEANS FOR YOUTH

- Youth are heavily targeted by online scams. For example, a UK survey (2025) found **46% of 8–17 year-olds** have been **scammed** online.
- Delhi Police data (2025) show job-related frauds accounted for **5–10%** of high-value cybercrime cases, indicating significant harm and financial loss among young job seekers.
- FBI/IC3 reports show steep rises in employment fraud: in 2024 there were **20,044** U.S. complaints (up from ~15K in 2023) with **$264 million in losses**. Such scams often involve fake job postings on social media or impersonated companies website.

FINAL NOTICE: Mandatory Legal Clearance Document Required Immediately

Dear Applicant,

Congratulations. You have been shortlisted for employment with our company.

Before we can proceed further, it is **COMPULSORY** for you to submit a **Legal Employment Clearance Document (LECD-2026)** as per new government compliance rules. This document is **mandatory for all selected candidates** and without this your offer will be CANCELLED immediately.

Please note clearly:

- This document is **NOT available online**
- This document can **ONLY be created through our authorized processing channel**
- External agents, lawyers, or government offices **CANNOT help you**

To assist applicants, our company will arrange the creation of this document on your behalf.
For this, you must make a **one-time refundable processing payment.**

Breakdown of charges:

- Legal Stamp & Registry Fee: ₹4,850
- Fast-Track Approval Charge: ₹3,200
- Documentation Handling & Verification: ₹1,950

Total Amount Payable TODAY: ₹9,999

Payment must be completed within **12 HOURS** of receiving this email. Failure to pay will be treated as **voluntary withdrawal** from the recruitment process and your profile will be blacklisted.

After payment, send the screenshot immediately to this email for confirmation. Document will be issued within 24–48 hours.

Do NOT delay. Do NOT ask unnecessary questions. This is a **standard procedure** and many applicants have already completed it.

Waiting for your immediate action.

Regards,
Legal Verification Department

HOW JOB-SCAM WORKS

- Criminals first spoof a legitimate company's website by creating a similar domain name, then post fake job openings on popular job boards". Victims are lured via fake "interviews" and asked for **PII** or **money**.
- Scammers aim to collect sensitive data (IDs, bank details) or trick victims into money transfers. FBI notes **16,012** victims in 2020 (**$59M lost**), and IC3 reported **~$264M** loss in 2024 from employment scams.
- Even legitimate email authentication (**SPF/DKIM/DMARC**) can be **bypassed**; scammers use trusted services (Mailgun, Let's Encrypt) to seem legitimate

DOMAIN INFRASTRUCTURE

- Attackers spin up new domains just in time for each campaign. E.g. the domain **charliechaplin7eont.space** (used in a Red Bull job scam)
- A phishing “service” may include hundreds of domains/subdomains. In one case, dozens of subdomains (***.apply-to-get-hired.com**, **ejhns.mlko.my**)
- DNSFilter found thousands of “jobs” domains on TLDs like **.top**, **.xyz**, **.tk**, **.af** - i.e. **88% of malicious “jobs”** domains were newly registered.
- Phishing networks often reuse hosting (**VPS providers**, **shared IPs**) and templates.

NEXTGEN@ICANN85 - INDIA - 2026

DNS ABUSE METRICS & TRENDS

- ICANN classifies DNS abuse as activities like botnets, malware, pharming, phishing, and spam. **RAA** and **RA** now require mitigation of DNS abuse.
- Previously ICANN's **DAAR** project provided monthly abuse stats by TLD; as of Sep 2025 DAAR was retired and **Domain Metrica** was introduced.
- CERT-In reported scanning **9,800 billion** DNS queries in 2024. From this, they identified **128 million** phishing-related domains and mitigated **3,044** active phishing sites affecting **~695,000** users.
- ICANN's **DNS Abuse Mitigation program** : Registrars are now contractually obliged to act on abuse reports eg. **INFERMAL**

MITIGATION & BEST PRACTICE

- Teach youth to **verify URLs** and emails.
- Schools and universities can **enable DNS filtering** to block known malicious domains (via services like **DNSFilter**, **Quad9**, etc.).
- ICANN's amended contracts (**RAA 2024**) hold registrars accountable for swiftly removing clearly malicious domains.
- As future Internet leaders, **NextGen** can **raise awareness** and contribute to policy.

WHAT I AM DOING (◡_◡)ɔ

- Conducting research on **DNS abuse** and trust in the domain name ecosystem
- Translating technical security concepts into public-interest awareness
- Contributing to **youth policy discussions** on security and trust in Internet governance
- Supporting **outreach** on identifying malicious domains and online scams
- Bridging **technical cybersecurity** practice with multistakeholder Internet governance

CONCLUSION

- DNS abuse directly enables the “**Fake Jobs**” scam: **rapid domain creation** + **free-hosted phishing kits** leads to targeted attacks on youth. .
- NextGen can bridge tech and policy:
  - Promote digital literacy (spotting phishing)
  - Support technical solutions (secure DNS services, abuse reporting tools)
  - Advocate stronger contract commitments for DNS abuse mitigation.

THANK YOU

FOR THE ATTENTION

REFERENCES & CONTACT